Signature and Timestamp in Electronic Document

Kazuya Miyazaki

Summary

In recent years business computerization and electronic commerce over the Internet has become popular, and according to this trend, there has been abrupt increase in electronic documents. Since it is quite easy to copy or process electronic documents compared to paper-based documents, it is difficult to guarantee authenticity of the electric documents: when, by whom and what is drafted. Thanks to development of PKI (Public Key Infrastructure) and constitution of Electronic Signature Law, the framework to guarantee the authenticity of electronic documents is being established in both of technical and legislative aspects. However, a digital signature at the center of the framework is of a problem in that not only it does not have a method to guarantee "when", but also it becomes unable to guarantee "by whom" and "what" as time advances.

One of the methods to solve this problem is Timestamp.

Timestamp is a scheme to guarantee existence of an electronic document at a particular point in time, and that the electronic document is not altered after the point in time. A timestamp is issued by a reliable third party called TimeStamping Authority. By using an accurate time as much as possible for the timestamp, or by disclosing hash values to the public media, such as journals or newspapers, it is possible to improve the reliability of the timestamp itself.

Timestamp is now drawing increasing attention, in such that it is adopted as a standard extended specification for the digital signature and a standard signature format for medical image information, and is expected to be used in a broad range of areas in the future.

Brief description of Timestamp (Description below the figure on the first page)

TimeStamping Authority, when transmitted hash values of the electronic document to which issuance of timestamps is desired, combines hash values and time information, and returns the data whereto signature by the TimeStamping Authority is attached as timestamps, and returns the timestamps. The accurate time information is obtained from GPS (Global Positioning System) satellites or the like. TimeStamping Authority periodically discloses the hash values to the public media, such as journals and newspapers to improve the reliability of the service.

1. Preface

In recent years business computerization and electronic commerce over the Internet has become popular, and according to this trend, there has been abrupt increase in electronic documents. Since it is quite easy to copy or process electronic documents

compared to paper-based documents, it is difficult to guarantee "when", "by whom" and "what" (documents with what kind of contents) is drafted (that is, guarantee for the authenticity of electric documents). Therefore, conventionally, there has been a need to exchange or preserve important documents in need of a legal proof in paper or microfiches, not in electronic documents.

Development of information security technology, especially, emergence of PKI, and constitution of Electronic Signature Law are changing such a situation. The digital signature in PKI is a technique that guarantees the creator or the sender (by whom) of the electronic documents, and that the contents of the electronic documents (what) are not altered. Electronic Signature Law is the law that provides legal grounds for the digital signature. Both PKI and Electronic Signature Law make it possible to secure the authenticity of electronic documents, and introduce the possibility to exchange or preserve important documents, such as administrative documents, medical records (medical chart), contracts, billing information, technical writing, and customer information, or the like.

However, the digital signature has temporal restriction as described below, therefore, the digital signature has a problem in that it is incapable of guaranteeing not only "when", but also "by whom" and "what" as time advances.

Timestamp is a way to solve this problem.

This document introduces a scheme of the digital signature, which is one of the representative methods of realizing electronic signature, problems of the digital signature, necessity and a scheme of Timestamp, and a prospect in the future.

2. PKI and The digital signature

It is decided that "Law Concerning Electronic Signatures and Certification Services", so-called "Electronic Signature Law" will be enforced from this coming April 1, 2001. Electronic Signature Law sets the regulations that information recorded in electromagnetic records shall be assumed to be authentic provided that a specific electronic signature is appended to the information by the principal, which provides electronic documents with legal grounds for achieving validity equivalent to paper-based documents by an electronic signature.

The electronic signature is defined as a measure taken with information recorded in electro-magnetic records in the aim of indicating a creator thereof, such as encryption, and a measure taken in a verifiable manner if alteration of the information has been performed. An electronic signature based on a public key is called the digital signature. Here, it is described a scheme of the digital signature according to PKI and how the digital signature guarantees authenticity.

PKI realizes the digital signature by using the public key cryptosystem. The public key cryptosystem is a system using a pair of two different keys (a public key and a secret key), where data encrypted by a public key can be only decrypted by using the

one and only secret key corresponding to the public key, and vice versa (encrypt with a secret key and decrypt with a public key). The secret key is privately stored in a rigorous manner, and the public key is disclosed to others. Certification Authority issues a certification (a public-key certification) to certify that the public key is correspondent to the secret key possessed by the principal, guarantees the relation.

Fig. 1 shows a scheme of the digital signature.

Next is described a procedure to generates and verifies the digital signature.

2.1 Generation Procedure of The digital signature

(1) A hash function is applied to an electronic document as an original text to generate a message digest. Here, the hash function is a function to convert a long-length original text into short-constant-length data (referred to as a message digest (MD) or a hash value, as well) and has a attribution to alter MD significantly even if the original text is altered only slightly.

(2) Generates a signature by encrypting MD with a secret key.

2.2 Validation Procedure of the Digital Signature

(1) Apply a hash value to the received original text to yield MD.

(2) Decrypt the received digital signature with a public key and yield MD.

(3) Determine if both the MDs agree.

Since the holder of the secret key is guaranteed and MD is altered in a case the original text is altered, therefore, if the both MDs agree, the following two facts are confirmed:

- Who generates the signature (the generator of the signature)
- For what the signature is signed (temper-proof function of the original text)

3. Problems in the Digital Signature

As described in the preceding section, the digital signature guarantees by whom and for what contents the signature has been appended. Here, what connects the signature and the signer is the certification. The certification has in fact a validity period and is subject to a "revocation" when the certification loses its validity before expiry of the validity period. When the certification revokes, the grounds for guaranteeing link among the secret key, the public key and a person as basis of the digital signature are lost. Additionally, the digital signature does not have a means to guarantee an accurate generated time (it is easy to embed a false time by manipulating a system clock in a personal computer whereon generating software runs), therefore, it is impossible to guarantee "when", and to confirm whether or not the digital signature is generated within the validity period or before the revocation, as well.

Thus, the digital signature is deemed to be valid only in the term within the validity period of the certification and before the revocation, and in consideration of the validity period normal certification being about a couple of years, the digital signature is quite transient. Then, if we try to store electronically the documents required to be saved

legally for a long term (for instance, five years for medical records, ten years for account books, 1 to 30 years for administrative documents), it is impossible to guarantee whether the documents are authentic or altered with the digital signature.

The problems are pointed out in Europe, as well, by EESSI (European Electronic Signature Standardization Initiative), and extended specifications of the digital signature using timestamps are proposed in the standardization activities by ETSI (European Telecommunications Standards Institute) and IETF (Internet Engineering Task Force) to solve these problems.

4. Timestamp

Timestamps are like stamps on mails, which guarantee the following two facts for the electronic documents:

- The electronic documents existed at a particular point in time
- The electronic documents are not altered after the point in time

However accurate a time is labeled, the label indicated by mere electronic data can be easily altered. The timestamps need some schemes to prevent such alteration, and some schemes are proposed. Here, it is explained a scheme whose standardization is underway in IETF.

The procedure in the scheme is as follows:

(1) A requesting party who requests issuance of the timestamps transmits hash values of electronic data to be appended to the timestamps to TimeStamping Authority.

(2) TimeStamping Authority binds time information (a GPS time signal is used usually to obtain an accurate time) to the received hash values, generates the digital signatures, and transmits the generated digital signatures together with the hash values and the time information as the timestamps to the requesting party.

TimeStamping Authority may periodically disclose the hash values to enhance the reliability of the timestamps. Here, some of the hash values obtained from the requesting party are concatenated, and the hash values obtained from the concatenated data are placed in journals and newspapers. As described in the section 2, the hash values are data alternating the original text, and by releasing the hash values, it is made possible to guarantee the existence of the original texts, which are the source of the hash values. The relation between the released time and the time indicated by the timestamps is verifiable, and by operating in a manner so that inconsistency does not occur between the times, the reliability of the timestamps is enhanced.

5. Conclusion

Since Timestamp resolves the problems in the digital signature and guarantees the validity of the digital signature, there has been a consideration of extended specifications of the digital signature using the timestamps, as well as an attempt to

define the digital signature format using Timestamp as extended specifications of the format of "Digital Imaging and Communication in Medicine" by DICOM (Digital Imaging and Communications in Medicine), which examines the formats concerning medical imaging. Additionally, since Timestamp can guarantee the existence of electronic documents and data at a particular point in time by itself, it is possible, for example, to claim a priority of an intellectual property when a timestamp has been obtained for technical information. Services having such a point have been already developed in U. S.

As stated above, Timestamp is now drawing increasing attention, and is expected to be used in a broad range of areas in the future.

Denshi Bunsho ni Okeru Shomei to Time Stamp

電子文書における署名とタイムスタンプ

宮崎一哉*

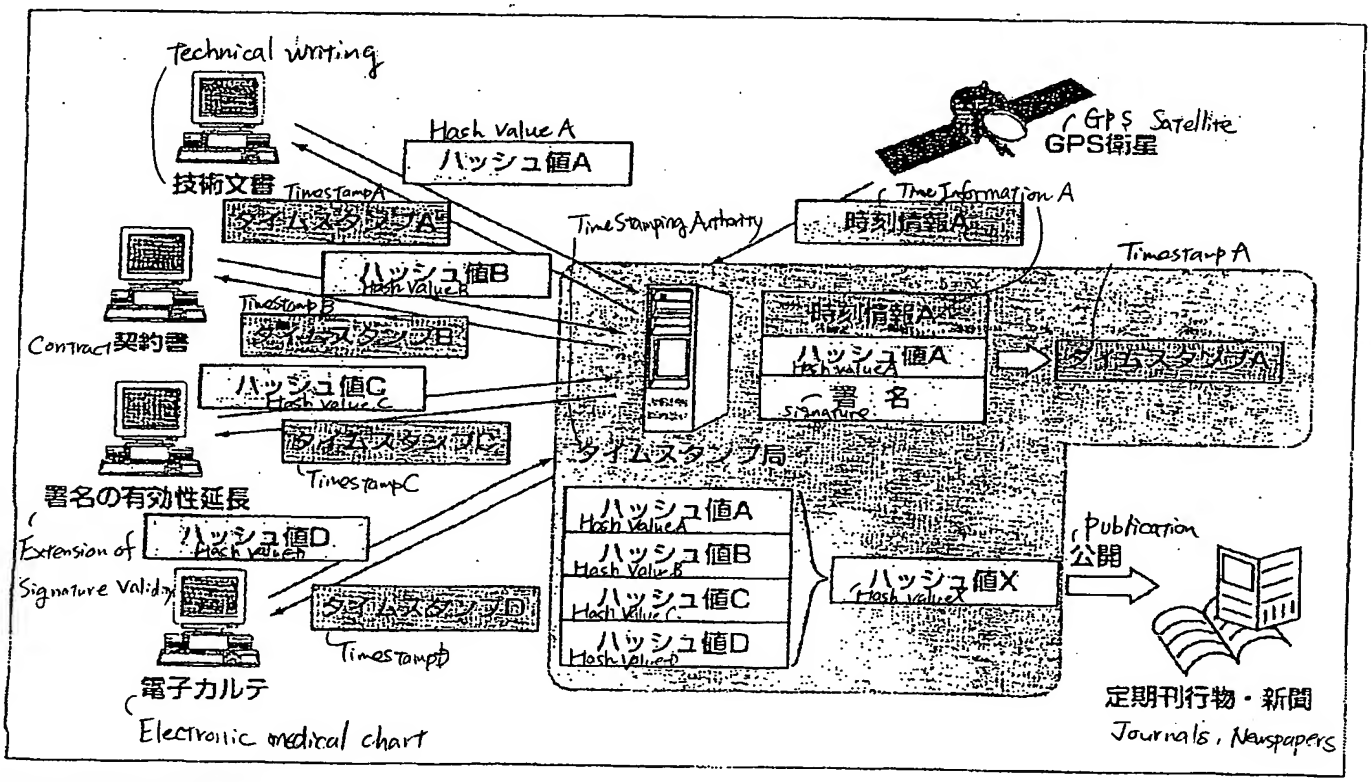
要旨

近年，業務の電子化やインターネット上での電子商取引が盛んに行われるようになり，これに伴って，電子文書が急激に増加している。ところが，電子文書は紙ベースの文書と比較して複製や加工が極めて容易であるため，いつ，だれが，何を作成したか，すなわち，真正性を保証することが難しい。PKI(Public Key Infrastructure：公開かぎ(鍵)基盤)の発展と電子署名法の成立によって電子文書の真正性を保証する枠組みが技術面・法制度面の両面から整いつつあるが，そこで中心となるディジタル署名は，"いつ"を保証する手段を持たないばかりか，時間の経過によって"だれ"及び"何"をも保証できなくなるという問題を抱えている。

これを解決する一つの手段がタイムスタンプである。

タイムスタンプは，電子文書のある時刻における存在と，その時刻以降，電子文書が改ざんされていないことを保証する仕組みである。タイムスタンプは，通常，信頼のおける第三者機関であるタイムスタンプ局によって発行される。このとき，タイムスタンプには可能な限り正確な時刻を利用するほか，ハッシュ値を定期刊行物や新聞などの大衆メディアに公開することにより，タイムスタンプ自体の信頼性を高めることができる。

ディジタル署名の標準拡張仕様や医用画像情報の標準署名フォーマットにタイムスタンプが採用されるなど，現在，タイムスタンプに対する注目度は高まっており，今後，幅広い分野において利用されることが予想される。



タイムスタンプの概要

タイムスタンプ局に対してタイムスタンプを取得したい電子文書のハッシュ値を送付すると，タイムスタンプ局は，ハッシュ値と時刻情報を結合し，タイムスタンプ局の署名を付けたデータをタイムスタンプとして送り返す。正確な時刻情報はGPS(Global Positioning System)衛星などから取得する。タイムスタンプ局は，定期的にハッシュ値を定期刊行物や新聞などの大衆メディアに公開することにより，サービスの信頼性を高める。

*情報技術総合研究所

1. まえがき

近年，業務の電子化やインターネット上での電子商取引が盛んに行われるようになり，これに伴って，電子文書が急激に増加している。ところが，電子文書は紙ベースの文書と比較して複製や加工が極めて容易であるため，"いつ""だれが""何"(どのような内容の文書を)を作成したかを保証すること(電子文書の真正性の保証という。)が難しい。このため，従来は，法的な証明力が求められるような重要な文書を，電子文書としてではなく，紙やマイクロフィッシュとして交換又は保管せざるを得なかった。

情報セキュリティ技術の発展，特にPKIの登場と電子署名法の成立が，この状況を変えつつある。PKIにおけるディジタル署名は，電子文書の作成者や発信者(だれ)を保証し，内容が改ざんされていないこと(何)を保証する技術である。電子署名法はディジタル署名に法的な根拠を与える法律であり，両者の存在によって電子文書の真正性が確保でき，行政文書，診療録(カルテ)，契約書，課金情報，技術文書，顧客情報といった重要な文書の電子文書による交換や保管等の可能性が開けてきた。

ところが，ディジタル署名には後述するような時間的制約が存在するため，"いつ"を保証できないばかりか，時間の経過により，"だれ"及び"何"をも保証できなくなるという問題を抱えている。

これを解決する手段がタイムスタンプである。

本稿では，電子署名の代表的な一実現方式であるディジタル署名の仕組み，ディジタル署名の問題点，タイムスタンプの必要性と仕組み，そして今後の展望を紹介する。

2. PKIとディジタル署名

来る2001年4月1日に「電子署名及び認証業務に関する法律」，いわゆる電子署名法が施行されることが決定した。この電子署名法は，電磁的記録に記録された情報について本人による一定の電子署名がなされているときは真正に成立したものと推定する旨の規定を設けるもので，電子文書が電子署名によって紙文書と同等な効力を持つための法的な根拠を与えられることになる。

電子署名とは，"電磁的記録に記録された情報について作成者を示す目的で行う暗号化等の措置で，改変があれば検証可能な方法によって行うもの"と定義される。公開鍵に基づく電子署名をディジタル署名という。ここでは，PKIに基づくディジタル署名の仕組みを説明し，ディジタル署名が真正性をいかに保証するかを説明する。

PKIでは，公開鍵暗号方式を用いてディジタル署名を実現する。公開鍵暗号方式は二つの異なる鍵のペア(公開鍵と秘密鍵)を利用する方式で，公開鍵で暗号化したデータはそれに対応するただ一つの秘密鍵を利用してのみ復号でき，その逆(秘密鍵で暗号化して公開鍵で復号する。)も同様である。秘密鍵は個人で厳重に保管し，公開鍵は他者に公開する。このとき，認証局は，公開鍵が本人の所有する秘密鍵に対応していることを証明するための証明書(公開鍵証明書)を発行し，その結び付きを保証する。

図1にディジタル署名の仕組みを示す。

次にディジタル署名の生成と検証の手順を示す。

2.1 ディジタル署名の生成手順

(1) 原文である電子文書にハッシュ関数を適用し，メッセージダイジェストを生成する。なお，ハッシュ関数は長い原文を短い固定長のデータ(メッセージダイジェスト(MD)，ハッシュ値ともいう。)に変換する関数であり，原文が少しでも変わるとMDが大きく変化するという性質を持つ。

(2) MDを秘密鍵で暗号化し，署名を生成する。

2.2 ディジタル署名の検証手順

(1) 受け取った原文にハッシュ関数を適用し，MDを生成する。

(2) 受け取ったディジタル署名を公開鍵で復号し，MDを生成する。

(3) 両MDが一致するかどうかを判定する。

秘密鍵の所有者が保証されること，原文が改ざんされるとMDが変化することから，両MDが一致した場合，次の二つの事実が確認できることになる。

- だれが署名を生成したか(署名生成者)
- 何に対して署名を施したか(原文の非改ざん性)

3. ディジタル署名の問題点

前節に示したように，ディジタル署名によってだれがどのような内容に対して署名したかを保証できる。このとき，署名と署名者を結び付けているのは証明書である。実はこの証明書には，有効期限が存在するばかりか，有効期限内に有効性を失う"失効"という事態が起こり得る。証明書が

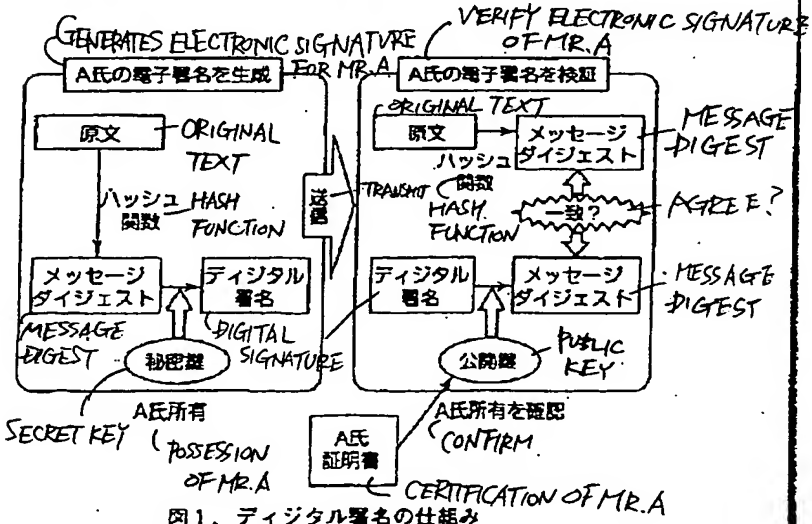


図1．ディジタル署名の仕組み

FIG 1. SCHEME OF DIGITAL SIGNATURE

有効性を失うと，ディジタル署名のベースとなる秘密鍵や公開鍵と人物の結び付きを保証する"よりどころ"を失う。また，ディジタル署名には正確な生成時刻を保証する手段を持たない(生成ソフトの動作するパソコンのシステム時計を操作することによって簡単に虚偽の時刻を埋め込めてしまう。)ため，"いつ"を保証できないばかりか，有効期限後には，そのディジタル署名が有効期限内又は失効前に生成されたのか否かを確かめることすらできなくなってしまう。

つまり，ディジタル署名が確実に有効であるとみなせる期間は，証明書の有効期限内でかつ失効前までの間であり，通常の証明書の有効期限が数年であることを考えるとディジタル署名はごく短命であるといえる。これでは，法的に長期の保存が要請される文書(診療録5年，商業帳簿10年，行政文書1～30年など)を電子的に保管しようとしたとき，それが真正なものであるのか又は改ざんされたものであるのかをディジタル署名では保証できないことになる。

この問題は欧州のEESSI(European Electronic Signature Standardization Initiative)でも指摘されており，この問題を解決するためのタイムスタンプを利用したディジタル署名の拡張仕様がETSI(European Telecommunications Standards Institute)，IETF(Internet Engineering Task Force)などの標準化活動において提案されている。

4. タイムスタンプ

タイムスタンプとは，郵便物に対する消印のようなものであり，電子文書に対して次の二つの事実を保証する。

- ある時刻に電子文書が存在したこと
- それ以降，電子文書が改ざんされていないこと

いくら正確な時刻を刻印しても単なる電子データで示したラベルでは容易に改ざんされてしまう。タイムスタンプにはそれができないような工夫が必要であり，幾つかの方式が提案されている。ここでは，IETFで標準化が進められている方式を紹介する。

この方式は，hash-and-sign methodと呼ばれる方式であり，信頼のおける第三者機関であるタイムスタンプ局の存在を想定する。

この方式における手順は次のとおりである。

(1) タイムスタンプの発行を要求する要求者がタイムスタンプを付加する対象となる電子データのハッシュ値をタイムスタンプ局に送付する。

(2) タイムスタンプ局は，受け取ったハッシュ値に時刻情報(通常は正確な時刻を得るためにGPSの時刻信号を利用する。)を結合し，そのディジタル署名を生成し，ハッシュ値，時刻情報とともに生成したディジタル署名をタイムスタンプとして要求者に送付する。

タイムスタンプ局は，タイムスタンプの信頼性を高めるために，ハッシュ値の公開を定期的に行う場合がある。この際，タイムスタンプ要求者から得たハッシュ値を幾つか連結し，その連結データから得たハッシュ値を定期刊行物や新聞などに掲載する。2章でも述べたように，ハッシュ値は原文を代替するデータであり，ハッシュ値を公開することにより，ハッシュ値の元となった原文が存在したことを証明することが可能となる。タイムスタンプに示された時刻と公開時刻の関係は検証可能であり，その間に矛盾を生じないように運用することにより，タイムスタンプの信頼性を高めることができる。

5. むすび

ディジタル署名の問題点を解決し有効性を長期間にわたって保証するために，タイムスタンプを利用した拡張仕様が検討されているほか，医用画像に関する規格を検討するDICOM(Digital Imaging and Communications in Medicine)でも"医用におけるディジタル画像と通信"規格の拡張仕様としてタイムスタンプを利用したディジタル署名フォーマットを規定しようとしている。また，タイムスタンプは単独で電子文書やデータのある時刻における存在を保証できるため，例えば技術情報に対してタイムスタンプを取得していれば知的財産の優先権主張が可能になると考えられている。米国では既にこのようなねらいを持ったサービスが展開されている。

このようにタイムスタンプへの注目度は高まりつつあり，今後，幅広い分野において利用されることが予想される。

参考文献

(1) 片木孝至，池端重樹，竹田栄作：暗号・セキュリティ技術の現状と展望，三菱電機技報，72，No.5，390－395 (1998)

(2) Nilsson, H., Eeche, P., Medina, M., Pinkas, D., Pope, N.: Final Report of the EESSI Expert Team, EESSI (1999)

(3) ETSI Standard: ETSI ES 201 733 Electronic Signature Formats, ETSI (2000)

(4) ETSI TC-SEC, Pinkas, D., Ross, J., Pope, N.: Electronic Signature Formats for Long Term Electronic Signature, IETF S/MIME WG (2000)

(5) DICOM Standard: Security Enhancements 2－Digital Signatures, Supplement 41, Working Draft Version 0.7 (2000)